複数のシスコ製品での Snort イーサネット フレーム デコーダのサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-snort-ethernet-dos-HGXgJH8n

初公開日 : 2021-03-03 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : No workarounds available

Cisco バグ ID : CSCvu88170

CVE-2021-1285

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

複数のシスコ製品は、Snort検出エンジンのイーサネットフレームデコーダ(EFH)の脆弱性の影響を受けます。これにより、認証されていない隣接する攻撃者がサービス拒否(DoS)状態を引き起こす可能性があります。

この脆弱性は、イーサネットフレームの処理時にエラー状態が不適切に処理されることに起因します。攻撃者は、該当デバイスを介して悪意のあるイーサネットフレームを送信することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスのディスク領域を使い果たしてしまい、管理者がデバイスにログインできなくなったり、デバイスが正しく起動できなくなる可能性があります。

注：この状況から復旧するには、手動による操作が必要です。この状況のデバイスの復旧については、Cisco Technical Assistance Center（TAC）にお問い合わせください。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-ethernet-dos-HGXgJH8n

該当製品

脆弱性のある製品

この脆弱性は、リリース2.9.17より前のすべてのオープンソースSnortプロジェクトのリリースに影響を与えます。オープンソースSnortの詳細については、SnortのWebサイトを参照してください。

シスコ製品への影響

IOS XE 用の Cisco UTD Snort IPS エンジンソフトウェアまたは IOS XE SD-WAN ソフトウェア用の Cisco UTD エンジンの脆弱なリリースを実行していて、イーサネットフレームを Snort 検出エンジンにパスすように設定されている場合、この脆弱性は次のシスコ製品に影響します。

- 1000 シリーズ サービス統合型ルータ（ISR）
- 4000 シリーズ サービス統合型ルータ（ISR）
- Catalyst 8000V エッジソフトウェア
- Catalyst 8200 シリーズ エッジ プラットフォーム
- Catalyst 8300 シリーズ エッジ プラットフォーム
- Cloud Services Router 1000V シリーズ
- サービス統合型仮想ルータ（ISRv）

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

脆弱性を含んでいないことが確認された製品

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Catalyst 8500 シリーズ エッジ プラットフォーム
- Catalyst 8500L シリーズ エッジ プラットフォーム
- Firepower Management Center（FMC）ソフトウェア
- Firepower Threat Defense(FTD)ソフトウェア[1]
- Meraki MX セキュリティアプライアンス

1. Cisco FTDソフトウェアに影響を与える関連する脆弱性は、Cisco Firepower Threat Defenseソフトウェアのインラインペア/パッシブモードの Denial of Service(DoS)の脆弱性として以前に解決され、公開されています。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコでは、このアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成は新規リリースでも継続して適切なサポートが受けられることを確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表に示すように、該当する修正済みのソフトウェアリリースにアップグレードすることをお勧めします。

Cisco IOS XE ソフトウェアおよび Cisco IOS XE SD-WAN ソフトウェア

IOS XE 用の Cisco UTD Snort IPS エンジンソフトウェアおよび Cisco UTD Engine for IOS XE SD-WAN Software[1]	この脆弱性に対する最初の修正リリース

16.12 より前	修正済みリリースに移行します。
16.12	16.12.5
17.1	修正済みリリースに移行します。
17.2	修正済みリリースに移行します。
17.3	17.3.3
17.4	17.4.1a

1.リリース17.2.1以降、Cisco IOS XEソフトウェアとCisco IOS XE SD-WANソフトウェアは同じイメージファイルを共有します。

オープンソースの Snort

オープンソースの Snort プロジェクトバージョン 2.9.17 以降には、この脆弱性に対する修正が含まれています。オープンソースの Snort の詳細については、Snort の Web サイトを参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-ethernet-dos-HGXgJH8n

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース	—	最終版	2021-MAR-03

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンド

ユーザを対象としています。